Title (en)

METHODS FOR SHARING AND USING A SECRET

Title (de)

VERFAHREN ZUR TEILUNG UND GEMEINSAMEN NUTZUNG EINES GEHEIMNISSES

Title (fr)

PROCÉDÉS DE PARTAGE ET D'UTILISATION D'UN SECRET

Publication

EP 3422239 A1 20190102 (FR)

Application

EP 18179657 A 20180625

Priority

FR 1755988 A 20170629

Abstract (fr)

Un premier dispositif (D1) souhaite partager un secret (S) avec un second dispositif (D2) supposé stocker un logiciel prédéfini. Le premier dispositif (D1) obtient une liste d'adresses aléatoires (L@) parmi un ensemble d'adresses correspondant au logiciel que le second dispositif (D2) est supposé stocker, et récupère le contenu supposé des adresses aléatoires de ladite liste, en utilisant un logiciel de référence (SW). Le premier dispositif (D1) calcule la clef de chiffrement symétrique, en appliquant une fonction de hachage prédéfinie sur le contenu récupéré, et transmet à destination du second dispositif (D2), en plus du secret chiffré grâce à la clef de chiffrement symétrique calculée, la liste d'adresses aléatoires (L@). Si le second dispositif (D2) dispose effectivement du logiciel attendu, le second dispositif (D2) est capable de retrouver la clef de chiffrement à partir de la liste d'adresses aléatoires (L@), et donc de déchiffrer le secret (S). Sinon, le second dispositif (D2) n'est pas capable de retrouver le secret (S), le déchiffrement donnant alors un résultat erroné.

IPC 8 full level

G06F 21/57 (2013.01); **G06F 21/44** (2013.01)

CPC (source: EP)

G06F 21/44 (2013.01); **G06F 21/57** (2013.01)

Citation (search report)

- [A] WO 2006106250 A1 20061012 - FRANCE TELECOM [FR], et al
- [A] US 2014006801 A1 20140102 - MULLEN SHAWN P [US], et al
- [A] WO 2013142943 A1 20131003 - IRDETO CANADA CORP [CA], et al

Cited by

CN113300842A

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

EP 3422239 A1 20190102; **EP 3422239 B1 20200205**; FR 3068498 A1 20190104; FR 3068498 B1 20190719

DOCDB simple family (application)

EP 18179657 A 20180625; FR 1755988 A 20170629